Federal Motor Carrier Safety Administration (FMCSA)

Information Technology Systems

Rules of Behavior – State Personnel

As a user of the Federal Motor Carrier Safety Administration Information Technology (FMCSA IT) Systems, I understand that I am personally responsible for the use and any misuse of my system account and password. I also understand that by accessing a U.S. Government information system that I must comply with the following requirements:

1. FMCSA IT systems are intended for official government use only.
2. FMCSA IT systems may not be used for commercial purposes, for financial gain, or in support of "for profit" non-government activities.
3. The government reserves the right to monitor the activity of any machine connected to its infrastructure.
4. FMCSA IT systems are the property of the Federal government. FMCSA manages the data stored on these systems for the benefit of all authorized users and owns all email messages, even those deemed personal.
5. Sensitive information (FOIA exempt or Personally Identifiable Information) may not be transmitted at a level higher than what the system is approved for.
6. Information that was obtained via FMCSA IT systems may not be divulged outside of government channels unless prior approvals by authorizing officials are granted.
7. Users of FMCSA IT systems may not communicate FMCSA information to external news groups, bulletin boards, or other public forums without permission.
8. Any activity that would discredit FMCSA, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material is not permitted.
9. Any activity that violates Federal laws for information protection (e.g., hacking, spamming, etc) is not permitted.
10. FMCSA IT system accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism **must never** be shared or stored **in printed form** any place accessible. If stored **digitally**, a password must not be stored in a clear-text or readable format.
11. Each FMCSA IT system has password format requirements and a password expiration policy. Although there are variations between systems, passwords which are at least 8 alphanumeric characters in length, and contain at least two letters and three numbers or special characters (@, $, #, etc.) will normally meet the requirement. Typically, passwords must be changed every 90 days (30 days for Administrator accounts).
12. Virus prevention tools must be installed and kept current on any and all machines from which FMCSA IT systems are accessed.

13. Any security problems or password compromises must be reported immediately to the FMCSA Information Systems Security Officer (ISSO) at FMCSA Headquarters (MC-RIS) and local FMCSA IT security personnel.
14. If Personally Identifiable Information (PII) is downloaded from FMCSA IT systems and stored on a laptop, the PII must be encrypted. The encryption hardware/software must be FIPS 140-2 compliant.
15. PII obtained from FMCSA IT systems must be encrypted if the PII is stored on mobile devices or removable storage media such as Compact Disks (CD) or Universal Serial Bus (USB) drives.
16. PII downloaded from FMCSA IT systems to laptops or workstations must be deleted when no longer required.

I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who:

a) Knowingly accesses an information system without authorization, or exceeds authorized access and obtains information that requires protection against unauthorized disclosure.

b) Intentionally, without authorization, accesses a Government information system and impacts the Government's operation, including availability of that system.

c) Intentionally accesses a Government information system without authorization, and alters, damages or destroys information therein.

d) Prevents authorized use of the system or accesses a Government information system without authorization, or exceeds authorized access, and obtains anything of value.

My signature below indicates that I have read, have understood, and will comply with the above stated requirements as a condition of maintaining active accounts with access to FMCSA IT systems. I also understand that failure to comply with these requirements may result in disciplinary action.

Name: _____ Telephone: _____

(Type or Print First MI Last)

Organization: _____ State: _____

Mailing Address Line 1: _____

Line 2: _____

City/State/Zip: _____

Telephone: _____

Office Symbol or Org Code: _____

Email Address: _____

Signature: _____ Date: _____